



Cybercrime

Von Onlinebetrug bis Datenklau



Stark für Sie.

www.ak-vorarlberg.at



Vorwort

Elektronischer Raub, Spam und Betrug: Die Kriminalität im Internet wächst rasant. Weltweit sollen die Einnahmen durch Internetverbrechen bereits höher sein als die durch illegalen Drogenhandel. Inzwischen reicht es oft schon, eine Webseite anzuklicken, um sich mit Schadsoftware zu infizieren. Immer mehr Seiten werden manipuliert und unterwandern dann die Rechner ihrer Besucher mit Programmen, die Daten zerstören oder ausspionieren können. Die Delikte reichen von Betrug über Geldwäsche bis zu Phishing und Hacking.

Die wichtigsten Infos und Tipps zu den häufigsten Internet-Ganereien finden Sie in diesem Folder. Sollten Sie darüber hinaus Fragen haben oder Hilfe benötigen, dann wenden Sie sich an unsere Experten in der AK-Konsumentenberatung. Sie helfen Ihnen gerne weiter.

Rainer Keckeis
AK-Direktor

Hubert Hämmerle
AK-Präsident

Cybercrime

Im Großen und Ganzen ist es so wie im wirklichen Leben – was dort verboten ist, ist im Internet auch illegal. Um einen kleinen Überblick zu geben, haben wir einige wichtige Punkte zusammengestellt.

Ab welchem Alter kann man sich strafbar machen?

Wenn man das 14. Lebensjahr vollendet hat, kann man für strafbare Handlungen zur Verantwortung gezogen werden. Bis zur Vollendung des 18. Lebensjahres gilt allerdings das Jugendstrafrecht, welches geringere Strafausmaße (meist die Hälfte der Erwachsenenstrafen) vorsieht.

Pornografie im Internet

Bei vielen Seiten mit pornografischem Inhalt finden sich auf der Startseite Hinweise, dass diese nur von Personen über 18 Jahre besucht werden dürfen. Manchmal muss man auch auf Buttons mit Formulierungen wie „über 18“ klicken. Das dient vor allem der Absicherung der Anbieter, sich nicht strafbar zu machen.

Anders ist es, wenn sich auf einer solchen Seite illegale Bilder befinden, in erster Linie Kinderpornografie. Hier ist bereits der Besitz strafbar. Besitz liegt dann vor, wenn eine solche Darstellung auf dem eigenen Computer gespeichert wird. In der Regel werden die Elemente einer Webseite schon beim bloßen Ansehen temporär auf der Festplatte gespeichert – bereits das kann als Besitz eines Bildes gelten. Kinderpornografie umfasst seit 2004 auch die Darstellung sexueller Handlungen an Personen unter 18 Jahren oder von Personen unter 18 an sich selbst, an anderen oder an Tieren, sofern es sich um reißerische Darstellungen („harte Pornografie“) handelt.

Pornografische Darstellungen mit Kindern unter 14 Jahren sind immer verboten. Es reicht bereits der Eindruck, dass es zu einer solchen Handlung gekommen ist. Beim bloßen Besitz von Kinderpornografie gilt ein Strafrahmen von bis zu einem Jahr, handelt es sich um Aufnahmen Unmündiger (unter 14) beträgt der Strafrahmen zwei Jahre Gefängnis. Diese Strafe kann sich auf bis zu drei Jahre erhöhen, wenn man Kinderpornografie herstellt oder auch nur anderen zugänglich macht.

Wer auf Kinderpornografie im Internet aufmerksam wird, kann sich anonym an www.stopline.at wenden.

Online-Betrug

Sie ersteigern bei einer Online-Auktion einen PC. Der Verkäufer streicht den Kaufpreis ein, obwohl der PC gar nicht existiert oder zumindest nicht geliefert wird. Ein Betrug liegt dann vor, wenn jemand einen anderen täuscht, um so einen Vermögensvorteil zu bekommen. Bedeutsam ist hier natürlich in erster Linie, ob und wie man das Produkt doch noch bekommen kann oder wie man sein Geld zurückerhält. Die Androhung einer Strafanzeige kann durchaus ein probates Druckmittel sein. Es liegt aber nicht automatisch ein Betrug vor, wenn man eine Sache nicht geliefert bekommt. Entscheidend ist, dass der Verkäufer von vornherein weiß, dass er gar nicht liefern kann oder will und trotzdem abkassiert.

„Phishing“

Eine besondere Form des Online-Betrugs ist das so genannte „Phishing“. Dabei versuchen Kriminelle mittels gefälschter Websites und E-Mails die Passwörter von Internet-Benutzern für Online-Konten, eBay- oder PayPal-Accounts oder Ähnliches herauszufinden.

Der User erhält meist eine täuschend echte E-Mail, mit der er oder sie aufgefordert wird, auf einen Link zu klicken und sich in seinen Account einzuloggen, beispielsweise um dort die Userdaten zu aktualisieren. Die Webseite, auf die der Link verweist, ist aber ebenfalls gefälscht und wenn man versucht sich dort einzuloggen, teilt man den Betrügern seine Accountdaten mit. In kürzester Zeit ist dann z. B. das Online-Konto leer geräumt.

Nachdem diese Fälschungen täuschend echt sind, sollte man mit Accountdaten besonders sensibel umgehen.

Dazu ein paar Tipps:

- ▶ Es gehört NICHT zum üblichen Verfahren von Banken, Onlineshops oder Auktionshäusern, sensible Daten der Nutzer via E-Mail abzufragen.
- ▶ Ignorieren Sie E-Mails, in denen zur Preisgabe von Daten und Passwörtern aufgefordert wird, auch wenn der angezeigte Absender bekannt ist. Meist strotzen solche betrügerischen E-Mails vor Rechtschreib- und Grammatikfehlern, um durch die Spamfilterkontrolle zu gelangen.
- ▶ Oft hilft auch nur ein Anruf bei der Hotline des jeweiligen Dienstleisters um herauszufinden, ob die E-Mail legitim ist oder nicht. Meist ist sie das nicht ...
- ▶ Persönliche Daten oder Accountinformationen sollten weder im Chat noch im Messenger-Service bekannt gegeben und auch nicht per Mail verschickt werden. Bei der Passwortwahl sollte man leicht zu erratende Kennwörter wie regelmäßige oder bekannte Zahlen, Geburtstage, Telefonnummern usw. vermeiden. Am besten ist eine Kombination von Buchstaben und Zahlen.
- ▶ Passwörter – wenn möglich – regelmäßig ändern.
- ▶ Bei der Eingabe von Daten immer auf SSL-Verschlüsselung achten. Die SSL-Verschlüsselung erkennt man daran, dass die Webseite mit <https://www> beginnt und im Browser das Vorhängeschloss geschlossen angezeigt wird.



- ▶ Wer eine zweifelhafte Internetseite besucht und seine Daten preisgegeben hat, sollte sofort das Passwort ändern und eine Sperre der TANs beim Onlinebankkonto veranlassen.

Geldwäsche

Vor allem aus Osteuropa erreichen Konsumenten immer wieder Spam-Mails mit verlockenden Verdienstmöglichkeiten. Dazu muss lediglich das eigene Bankkonto für Geld-Transaktionen zur Verfügung gestellt werden. Die „Geschäfte“ laufen dann immer nach dem gleichen Muster ab: Es wird Geld auf das Bankkonto überwiesen, der Kontoinhaber muss die Summe per Western Union weiterschicken und wird dafür angeblich reichlich entlohnt. Tatsache ist: Die Banküberweisung wird in der Regel storniert, der Kontoinhaber verliert sein Geld, das er per Western Union weitergeschickt hat und macht sich überdies der Geldwäsche strafbar.

Scheckbetrug

Ähnlich wie bei der Geldwäsche verhält es sich beim Scheckbetrug: Die Internet-Gauner suchen sich Leute, die Konsumprodukte, z. B. gebrauchte Autos, verkaufen wollen. Für die Bezahlung des Gebrauchtwagens wird dann ein Scheck mit einem weit überhöhten Betrag ausgestellt. Den Differenzbetrag zum Preis des Autos möge man doch per Western Union weiterschicken, wird man vom freundlichen Käufer gebeten. Wenn der Scheck schlussendlich platzt – und das tut er mit Sicherheit – ist beides weg: Das Auto und das Geld, das per Western Union überwiesen worden ist.

Virenprogramme

Sie erhalten ein Virenprogramm als Mail-Anhang, welches Ihre Festplatte löscht. Das fällt unter Datenbeschädigung. Allerdings nur, wenn der Absender das Löschen beabsichtigt hat. Versendet sich das Virenprogramm vor dem Löschen noch automatisch an alle Kontaktadressen in Ihrem Mail-Programm und löscht auch die Festplatten Ihrer Bekannten, sind Sie nicht strafbar.

Hacking

Auch das unerlaubte Eindringen in fremde Computersysteme kann strafbar sein. Voraussetzung ist, dass Sicherheitsvorkehrungen des Systems verletzt wurden. Weiters ist Hacking nur dann gerichtlich strafbar, wenn sich der Täter oder die Täterin einen Vermögensvorteil verschafft oder den Betreiber des Systems schädigen will. Auch die schwere Störung eines fremden Computernetzwerkes ist als Datenbeschädigung und Störung der Funktionsfähigkeit eines Systems strafbar. Strafbar ist auch das Umgehen von Zugangsbeschränkungen oder technischen Sperren. Der Strafraum beträgt bis zu sechs Monate.

Das Verwenden von Hacking-Tools oder Computerviren ist als so genannter Missbrauch von Computerprogrammen seit 2003 im österreichischen Strafrecht genannt. Das Abfangen von Daten, die über Computernetzwerke übermittelt werden und nicht für Sie bestimmt sind, ist gleichfalls verboten. Sowohl im Strafgesetzbuch als auch im Telekommunikationsgesetz gibt es weitere Strafbestimmungen, die es verbieten, fremde E-Mails zu lesen oder sonstige Daten über fremden Telekommunikationsverkehr anzusehen oder weiterzugeben. Auch im Internet gilt: Fremde Briefe oder Akten öffnet man nicht ohne Erlaubnis.

Wir sind für Sie da:

AK-Konsumentenberatung,
Widnau 2 – 4, 6800 Feldkirch,
Telefon 050/258-3000, Fax 050/258-3001
konsumentenberatung@ak-vorarlberg.at,
www.ak-vorarlberg.at/konsument

Impressum

Stand: April 2009
Herausgeber: AK Vorarlberg
Widnau 2 – 4, 6800 Feldkirch
Telefon 050/258-0, Fax 050/258-1001
kontakt@ak-vorarlberg.at, www.ak-vorarlberg.at
Druck: Bucher GmbH, Hohenems

Die vorliegende Broschüre wurde nach bestem Wissen verfasst. Dennoch kann keine Haftung für die Richtigkeit und Vollständigkeit sämtlicher Informationen übernommen werden. Die allgemeinen Informationen ersetzen im konkreten Einzelfall keine intensive rechtliche und persönliche Beratung.



Konsumentenberatung

Widnau 2 – 4, 6800 Feldkirch

Telefon 050/258-3000

Fax 050/258-3001

konsumentenberatung@ak-vorarlberg.at

www.ak-vorarlberg.at